

IN THE UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF MISSOURI
SOUTHWESTERN DIVISION

UNITED STATES OF AMERICA,)
)
)
)
)
v.)
)
MARK E. DREW,)
)
)
)
)

Case No. 14-05023-01-CR-SW-BP

**ORDER AND OPINION (1) ADOPTING MAGISTRATE JUDGE’S REPORT AND
RECOMMENDATION AND (2) DENYING DEFENDANT’S MOTION TO SUPPRESS**

Defendant has been indicted on one count of receiving or distributing child pornography. He filed a Motion to Suppress, (Doc. 22), contending the search warrant was legally infirm in a variety of respects. The Honorable David P. Rush, United States Magistrate Judge for this District, held a hearing on August 6, 2015, and he issued a Report on September 10, 2015 recommending that the Motion to Suppress be denied. (Doc. 42.) Defendant objects to Judge Rush’s Report and Recommendation (“the Report”). The Government has not responded to the Objection, and the time for doing so has passed. Local Rule 74.1(a)(2).

The Court has conducted a de novo review as required by 28 U.S.C. § 636(b)(1). In particular, the Court has reviewed the parties’ submissions before the hearing, the transcript from the hearing, the exhibits admitted during the hearing, and Defendant’s objections. Having conducted this review, the Court adopts the Report as the Order of the Court and denies the Motion to Suppress; the Court’s discussion is intended to augment, not supplant, the Report.

I. BACKGROUND

The Court focuses on those facts and events that are particularly relevant to Defendant’s Objections, and those events actually began in Russia. While investigating a report of a person

engaging in sexual misconduct with a minor, Russian officials learned that the target of their investigation posted photographs of him engaging in sex acts with a minor on a website in Russia. (This website has been referred to as “Website A” to avoid compromising the Russian authorities’ continuing investigation.) Russian authorities learned Website A was often used to host pictures of child pornography and obtained a warrant authorizing the seizure of Website A or its data. Individuals associated with Website A cooperated with the authorities to provide data responsive to the warrant. (Doc. 41, pp. 44-53.) Website A did not provide the entirety of its database but the Record does not specify what was not provided.¹

Russian authorities provided the FBI with information they obtained from Website A suggesting that a particular United States citizen had uploaded what appeared to be child pornography to Website A and was seeking to exchange pictures with others.² Russian authorities provided the FBI with the information in computer code, leaving it to the FBI to convert the code. (Doc. 41, p. 9.) The information included the “hash values” for the pictures the user posted; a hash value has been described as “a digital fingerprint of the photo” and any photograph taken has a unique hash value. (Doc. 41, p. 11.)³ The hash values were compared to hash values of photographs known to have been the product of child exploitation. Some (but not all) of the hash values posted by the user in question matched hash values in the FBI’s database; in this way, the FBI was able to identify some of the pictures posted by the user even though the

¹ It could be that Website A cooperated with Russian authorities by supplying all pictures that might constitute child pornography (as apparently sought by the Russian warrant) and omitting all benign pictures. “Website A is organized by different forums according to topic. Examples include topics such as ‘architecture,’ ‘travel,’ ‘family,’ and ‘autos.’ Each website forum contains albums posted and named by the registered website user that created the album.” (Exh. 2, ¶ 33.)

² Russian authorities have provided the FBI with information about other users as well, but that detail is not relevant to the Court’s discussion.

³ A photograph can be expressed in terms of a mathematical formula that is unique to that photograph. (Doc. 41, pp. 11-12.) Thus, two hash values can be compared; if they are the same, then they have been generated by the same photograph.

pictures themselves had not been supplied by the Russian authorities. Specifically, there were five photographs that appeared in the FBI's database, and these pictures have been described as "the Laura pictures." The user posted the Laura pictures in July 2010. (Doc. 41, p. 57.)

The data provided to the FBI also included the user name, which for most of the relevant time period was "maddog8in."⁴ The information also provided maddog8in's e-mail address at yahoo.com, and the FBI issued an administrative subpoena to Yahoo! to obtain the associated IP addresses. One of the IP addresses was more recent than the other; and an administrative subpoena was served on the issuer of that IP address (Cable One), which revealed Defendant as the recipient of that IP address.

A search warrant was sought by Charles Root, a police officer with the Joplin Police Department who also served as a Task Force Officer ("TFO") with the FBI's Violent Crimes Against Children Task Force. TFO Root's supporting affidavit, (Exhibit 2), included some details about the investigation and about Website A, and described how (1) maddog8in was identified as a user who created albums and posted pictures on Website A, (2) an administrative subpoena was issued to Yahoo! to obtain the IP addresses associated with maddog8in, and (3) how a subpoena was issued to Cable One to identify the person and address associated with the later of the two issued IP addresses. (Exhibit 2, ¶¶ 38-40.) The affidavit also stated that

five images [posted by maddog8in] depict the same female child that appears to be approximately 13 years old. The images depict the child in various forms of undress and posing suggestively for the camera. Four of the five images have the name, "Laura" in the title. One of the images . . . depicts the child lying on a couch with her arm over her head. She is naked from the waist down and a large birth mark is visible on her left hip. Her leg is crossed over herself, preventing full view of her vagina in this preview photo.

(Exhibit 2, ¶ 41.) The affidavit also describes comments posted by maddog8in, some of which expressed a desire to trade pictures with others, (*id.* ¶¶ 38, 41); the Record is not clear whether

⁴ The circumstances leading to the user changing the user name to "maddog7" are not relevant here.

any of these comments were posted with the pictures of Laura, but one comment states that “The vids from Laura when younger are nicer ;)” which strongly indicates that at least that comment was associated with a picture of Laura. (Exh. 2, ¶ 41.)

The affidavit suggested there was probable cause to believe several federal statutes had been violated, including statutes that prohibit the receipt or distribution of pictures of a minor engaging in sexually explicit conduct. 18 U.S.C. §§ 2252(a)(2), 2252A(a)(3). The Magistrate Judge agreed and issued a warrant. As a result of their search, law enforcement officers seized three computers, a flash drive, and a DVD; collectively, this equipment contained more than 350 images of child pornography. Defendant seeks to suppress this evidence, contending (1) the warrant was not supported by probable cause, (2) the affidavit supporting the warrant contained false or misleading information and omitted material information, and (3) the use of administrative subpoenas to obtain information from Yahoo! and Cable One violated Defendant’s Fourth Amendment rights.⁵

II. DISCUSSION

A. Probable Cause

“Issuance of a search warrant must be supported by probable cause, and the existence of probable cause depends on whether, in the totality of the circumstances, there is a fair probability that contraband or evidence of a crime will be found in a particular place. We accord great deference to a magistrate’s determination as to whether an affidavit establishes probable cause. Instead of reviewing an affidavit in a hypertechnical fashion, courts should apply a common sense approach.” *United States v. Rodriguez*, 711 F.3d 928, 936 (8th Cir.), *cert. denied*, 134 S. Ct. 715 (2013) (internal citations and quotations omitted). Reading TFO Root’s affidavit in this

⁵ Defendant presents these arguments in a different order, but the Court prefers to consider the arguments in this manner.

light, the Court concludes there was probable cause to justify the search. The affidavit did not specify when the Laura pictures were uploaded, but it provided information establishing maddog8in had accessed Website A from 2008 until just before the search warrant was executed. Thus, there was probable cause to believe there would be evidence further demonstrating Defendant uploaded the Laura pictures. Moreover, the affidavit contained information suggesting Defendant sought to trade pictures with other visitors to Website A through more direct channels (that is, without using Website A), thereby creating probable cause to believe there would be evidence of such trades on his computer. Defendant emphasizes the passage of time between the uploading of the Laura pictures and the search. However, “[t]here is no bright-line test for determining when information in a warrant is stale,” *United States v. Pruneda*, 518 F.3d 597, 604 (8th Cir. 2008), and the Court agrees with the Report’s conclusion that the nature of the crime and Defendant’s continued accessing of Website A suggests little likelihood that he had destroyed evidence on his computer. *See United States v. Lemon*, 590 F.3d 612, 614-15 (8th Cir. 2010).

Alternatively, suppression would not be warranted even if the affidavit failed to present probable cause because the search was executed in good faith reliance on a warrant. “Under the good-faith exception, evidence seized pursuant to a search warrant issued by a magistrate that is later determined to be invalid, will not be suppressed if the executing officer’s reliance upon the warrant was objectively reasonable.” *United States v. Proell*, 485 F.3d 427, 430 (8th Cir. 2007). Defendant invokes two exceptions to the good-faith exception, contending (1) the supporting affidavit contained false statements that misled the issuing Magistrate Judge and (2) the probable cause showing was so deficient that reliance on the warrant was entirely unreasonable. (Doc. 22, p. 28); *see also Proell*, 485 F.3d at 431 (citing *United States v. Leon*, 468 U.S. 897, 923 (1984)).

and listing exceptions). Defendant's invocation of the first exception essentially imports his second argument, and as discussed below the Court concludes there was no materially false or misleading information included in, or material information omitted from, TFO Root's affidavit. As to the second exception, for the reasons expressed above the Court concludes that even if the affidavit did not present probable cause it was reasonable for law enforcement to rely on the Magistrate Judge's decision to issue the warrant.

B. *Franks v. Delaware*

In *Franks v. Delaware*, the Supreme Court held that a defendant "may request a hearing to challenge a search warrant on the ground that the supporting affidavit contains factual misrepresentations or omissions relevant to the probable cause determination." *United States v. Arnold*, 725 F.3d 896, 898 (8th Cir. 2013) (citing *Franks*, 438 U.S. 154, 155-56 (1978)). The standards for obtaining a hearing are not relevant to this proceeding because a hearing was actually held. Thus, to prevail Defendant must demonstrate that TFO Root deliberately or recklessly included a false statement or omitted a truthful statement from the affidavit and that if the correct information had been included the affidavit would not have established probable cause. The Court agrees with the Report's conclusion that Defendant is not entitled to relief.

Defendant contends the affidavit was infirm in the following respects:

1. Its description of the picture was false because it described one of the Laura pictures as showing the subject with her "leg . . . crossed over herself, preventing full view of her vagina in this preview photo" when in reality the image did not show Laura's genitalia.
2. It omitted the fact that the people cooperating with the Russian authorities' execution of the Russian warrant on Website A's behalf were unknown to TFO Root, and he had no information about the trustworthiness, reliability or veracity of those individuals.

3. It omitted the fact that Website A did not provide all of its data from or about the site.
4. It omitted the fact that the first IP address had not been investigated to ascertain its physical location.
5. It omitted the fact that the Laura pictures were posted more than three years before the affidavit was prepared.
6. It wrongly implies that the comments described in the affidavit were associated with the Laura pictures.

The Court agrees with the Report that to the extent any of these characterizations are correct, none were material; that is, even if the affidavit included the allegedly “missing” information or had been amended to describe facts as Defendant views them, probable cause would have still existed. The Court adds the following observations regarding the first four issues:

1. The “more accurate” description of the Laura picture that Defendant advocates would have also supported the finding of probable cause. Moreover, having reviewed the Laura picture, the Court believes that if the Laura picture had been supplied with the affidavit, probable cause would have been established. Probable cause existed if there was probable cause to believe, *inter alia*, that the picture depicted Laura engaging in “sexually explicit conduct.” Sexually explicit conduct is statutorily defined to include “lascivious exhibition of the genitals *or pubic area* of any person.” 18 U.S.C. § 2256(2)(A)(v) (emphasis supplied). In addition to reviewing the Laura picture, the Court has reviewed the law regarding the definition of sexually explicit conduct. *E.g.*, *United States v. Kemmerling*, 285 F.3d 644, 645-46 (8th Cir.), *cert. denied*, 537 U.S. 860 (2002) (“[M]ore than mere nudity is required before an image can qualify as ‘lascivious’ within the meaning of the statute. A picture is ‘lascivious’ only if it is sexual in

nature. Thus, the statute is violated, for instance, when a picture shows a child nude or partially clothed, when the focus of the image is the child's genitals or pubic area, and when the image is intended to elicit a sexual response in the viewer."); *see also United States v. Horn*, 187 F.3d 781, 789-90 (8th Cir. 1999), *cert. denied*, 529 U.S. 1029 (2000); Eighth Circuit Model Instruction 6.18.2252A. The Court independently concludes that if the picture – the best proof of the picture's contents – had been included with TFO Root's affidavit, there would still have been probable cause to believe maddog8in posted a picture of a minor engaged in sexually explicit conduct.

2. Defendant's second argument essentially equates Website A's employees with confidential informants. "An informant's tip can be sufficient to establish probable cause if the informant has a track record of supplying reliable information or if the tip is corroborated by independent evidence." *United States v. Gabrio*, 295 F.3d 880, 883 (8th Cir. 2002) (quotations omitted). However, Website A did not provide information; it provided physical evidence. Website A provided computer files to Russian authorities, and Russian authorities provided those files to the FBI. Defendant cites no case law equating this situation to those involving confidential informants, and the Court holds the case law regarding informants does not apply here.

3. Defendant has not established that Website A failed to provide any data relating to him (as opposed to other users who did not post pictures that might constitute child pornography), much less the nature of any such omitted data. Therefore, he has not carried his burden of establishing that the omitted information would have affected the probable cause determination.

4. The Court agrees with the Report's conclusion that TFO Root's affidavit did not omit the fact that the first IP address was not investigated. (Doc. 42, pp. 8-9.) The Court also holds that

including a “more explicit” statement to this effect would not have altered the probable cause determination. Trying to find the former owner of the oldest IP address would not have likely produced information because the provider probably did not have the information any longer. (Doc. 41, p. 56.) Moreover, an IP address usually relates to a physical location, (Doc. 41, pp. 39, 77), and the probable cause determination required an assessment of where maddog8in was at the time of the search, not where maddog8in had been sometime in the past.

C. Administrative Subpoenas

The Court agrees with the Report’s analysis, particularly its reliance on the Eighth Circuit’s holding that a person does not have a privacy interest in subscriber information voluntarily supplied to an internet provider. *United States v. Wheelock*, 772 F.3d 825, 828-29 (8th Cir. 2014). The Supreme Court’s decision in *Riley v. California*, 134 S. Ct. 2473 (2014), does not dictate a different result because (1) *Wheelock* was decided more than five months after *Riley* and (2) the information sought by the administrative subpoenas in this case was far more limited than the information at issue in *Riley*.

III. CONCLUSION

For these reasons, the Court **OVERRULES** Defendant’s objections, (Doc. 47), **ADOPTS** Judge Rush’s Report and Recommendation, (Doc. 42), and **DENIES** the Motion to Suppress. (Doc. 22.)

IT IS SO ORDERED.

DATE: November 23, 2015

/s/ Beth Phillips
BETH PHILLIPS, JUDGE
UNITED STATES DISTRICT COURT